Case Western Reserve Law Review

Volume 66 | Issue 1

2015

Derivative-Consent Doctrine and Open Windows: A New Method to Consider the Fourth Amendment Implications of Mass Surveillance Technology

Alex Brown

Derivative-Consent Doctrine and Open Windows: A New Method to Consider the Fourth Amendment Implications of Mass Surveillance Technology

Contents

Introduction

Our lives are filled with open windows. Plenty of these windows are in our homes, schools, businesses, and other buildings, and they often have blinds on them that we can open or close, depending on our

comfort with what outsiders will get to see within the buildings. Not all windows are on buildings. Some of them are in our pockets. Some of them sit on our desks. Some of them sit in closed compartments of our cars, ready to navigate us to a new destination. These windows are electronic devices, and they can provide a myriad of information about our lives. While we voluntarily provide information to these devices in order for them to perform the functions we desire, consider the possibility of these devices seemingly acting on their own accord. Also consider whether the contents of messages sent through e-mail or social media to designated recipients are truly private. Imagining the startling image of a government agent reviewing your most intimate messages to your significant other provokes fear.

This Comment is designed to determine when, and what kinds, of information should be reviewable by government agents through individuals' voluntary actions. In order to do this, Part I reviews a recently decided case, *ACLU v. Clapper*,[1] analyzing how the case would be decided as a Fourth Amendment issue, had the Second Circuit Court of Appeals decided the case on that basis. Part II outlines three categories of Fourth Amendment jurisprudence, which will provide a helpful background to readers new to Fourth Amendment issues.

Part III determines the outcome of *Clapper* using the Fourth Amendment jurisprudence reviewed in Part II. Part IV reviews proposals to counter the pervasiveness of mass surveillance in American society, some of which come from the Supreme Court as well as academia. I also propose a solution, further delineated in Part Five. The Comment ends with a summary of the topics discussed and final thoughts on the overall subject.

This Comment will show that the bulk collection of metadata from telephone calls and other electronic communications are permissible under the Fourth Amendment of the United States Constitution without a warrant. However, disclosing the contents of communications to government agencies and operating devices without the consent of their owner constitutes searches requiring a warrant.

I. Case Summary

This Comment will begin by summarizing its subject case, *ACLU v. Clapper*.[2] Doing so provides necessary background but also demonstrates *Clapper*'s relevance in the overarching issue of mass surveillance in the United States. *Clapper* provides a springboard into difficult but necessary discussions about the constitutionality of domestic surveillance programs. The Second Circuit's decision in *Clapper* also provided

1. 785 F.3d 787 (2d Cir. 2015).

2. 785 F.3d 787 (2d Cir. 2015).

momentum for Congress to craft a legislative remedy for the federal government's metadata collection from telecommunications companies' phone records, a remedy which will be discussed further below as one possible non-judicial solution to mass surveillance, should society deem privacy and civil liberties to be a greater interest than security.[3]

A. Facts

Clapper decided whether the government may require telecommunications companies to transfer telephone metadata in bulk.[4] This begs the question, what is metadata? Defining what it is not provides a sigh of relief to many libertarians, for metadata does not include the voice content of telephone conversations. It does include other pertinent information, such as a call's length, the phone number the call came from, and the phone number dialed.[5] Occasionally, metadata reveals the identity of callers and the devices they use, through identity numbers related to phone equipment.[6] In other instances, how a call is routed through the telecommunications network may reveal a caller's general location, but when metadata provides this information, locational data is far less precise than that detected by cell sites.[7] Despite metadata's inability to replicate the most intimate information about a phone call—the contents of the conversation—it still may reveal a great deal of otherwise hidden information, such as intimate relationships, religious beliefs, perhaps even a person's mental health (all by identifying the individuals associated with phone numbers dialed, and the source of those numbers).[8]

Judge Gerald E. Lynch, writing the *Clapper* majority opinion for the Second Circuit, acknowledged similarities between information gathered from telephone metadata and more traditional sources, like the addresses on an envelope. But he distinguished telephone metadata from traditional identifying information by emphasizing the "vast new technological capability for large-scale and automated review and analysis."[9] Though Judge Lynch does not state this outright, he is likely referring to intelligence services pooling vast quantities of metadata and then searching the metadata for individuals the intelligence community is interested in. Metadata is valuable for this task since, in a world closely connected by mobile phones, it is "virtually impossible" for

3. *See infra* text accompanying note 38.

4. *Clapper*, 785 F.3d at 793.

5. *Id.*

6. *Id.* at 794.

7. *Id.*

8. *Id.*

9. *Id.*

individuals to avoid generating metadata through their normal routine.[10] After reviewing the importance and pervasiveness of metadata, Judge Lynch transitions to the facts.

The federal government determined that it could gather metadata on the basis of section 215 of the Patriot Act. This statute allows the FBI Director or his designee to "make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[11] A now-infamous Foreign Intelligence Surveill-ance Court (FISC) order required Verizon Business Network Services, Inc. to produce call records, on a daily basis, of all telephone calls made through its systems or services where one or both ends of the call are within the United States.[12] What makes this order infamous is that it was revealed to the world by ex-federal government contractor Edward Snowden in an article published by the British newspaper *The Guardian*.[13] The federal government later acknowledged that the Verizon order was a small part of a much larger program collecting bulk telephone data launched in May 2006.[14] This program began with an order, couched under section 215 of the Patriot Act, to produce "tangible things" that the federal government construed to mean telephone metadata.[15]

The Government explained the purpose of collecting bulk metadata: to fight terrorism.[16] Phone numbers believed by the government to be associated with a foreign terrorist, based on a "reasonable articulable suspicion," were searched within a massive database containing metadata to yield phone numbers in contact with the suspicious phone number, called a "seed."[17] A search would follow of all numbers found in the metadata to be in contact with the seed number, and searches of "the contacts of contacts of contacts of the original 'seed'" telephone

10. *Id.*

11. 50 U.S.C. § 1861(a)(1) (2012); *Clapper*, 785 F.3d at 795.

12. *Clapper*, 785 F.3d at 795–96.

13. *Id.* at 795. *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [http://perma.cc/42WP-3WGB].

14. *Clapper*, 785 F.3d at 796.

15. *Id.*

16. *See id.* at 797.

17. *Id.*

number occurred as well.[18] Responding to public pressure, President Barack Obama ordered the FISC to alter the telephone meta-data program in January 2014.[19]

President Obama made two changes to the telephone metadata program. First, he only allowed searches of the metadata of phone numbers in contact with the seed, or first suspicious phone number, thus prohibiting searches of the "contacts of contacts of contacts of the original 'seed'" number.[20] Judge Lynch described this as limiting the searches to "two, rather than three" hops.[21] The second change to the telephone metadata program required an FISC judge determine that the National Security Agency (NSA) satisfied the reasonable articulable suspicion standard before allowing a telephone number to be searched within the telephone metadata pool.[22]

B. Procedural Posture

The American Civil Liberties Union (ACLU), New York Civil Liberties Union (NYCLU), as well as current and former Verizon customers, sued the government officials administering the telephone metadata program on both statutory and constitutional grounds.[23] The complaint, filed in the Federal District Court for the Southern District of New York on June 11, 2013, requested that the court "declare that the telephone metadata program exceeds the authority granted by § 215, and also violates the First and Fourth Amendments to the [United States] Constitution."[24] About two months later, the plaintiffs asked for a preliminary injunction, which would halt the government's collection of metadata, quarantine the records already collected, and prohibit use of the records to perform queries into the phone numbers and other identifying information associated with the plaintiffs.[25] The government moved to dismiss the complaint on the same day.[26] On December 27, 2013, "the district court granted the government's motion to dismiss and denied plaintiffs' motion for a preliminary injunction," setting the stage for an appeal to the Second Circuit.[27]

18. *Id.*
19. *See id.* at 798.
20. *Id.* 797–98.
21. *Id.* at 798.
22. *Id.*
23. *Id.* at 799.
24. *Id.*
25. *Id.* at 799–800.
26. *Id.* at 800.
27. *Id.*

C. Second Circuit's Decision

Once *Clapper* arrived at the Second Circuit, some preliminary matters were disposed of prior to the court reaching the merits of the case. First, the Second Circuit held that the ACLU and fellow plaintiff-appellants had standing to sue because the "government's own orders demonstrate that appellants' call records are indeed among those collected as part of the telephone metadata program."[28] Appellants' injury was the initial collection of their telephone metadata through the Verizon order, rather than a subsequent search of the data.[29] The injury, seizure of metadata, is within the scope of the Fourth Amendment because it prohibits illegal searches and seizures.[30] After surviving a standing challenge, the appellants still had one preliminary issue to overcome before reaching the merits of their claims.

The Government next argued that Congress never intended to allow targets of section 215 orders from seeking judicial review. In doing so, the Government stated that statutes keeping the metadata program secret indicated an implied Congressional intent to prevent judicial review for those actually targeted by section 215, such as telecommunications companies.[31] The Second Circuit disagreed. It stated that "clear and convincing" or "fairly discernible" evidence must suggest Congress intended to preclude judicial review, and no such evidence was found.[32] The court further concluded that it found no unexpressed intention to withdraw judicial rights granted in a generally applicable Administrative Procedure Act statute.[33] Finally, the court proceeded to the merits.

The court, confronted with a statutory issue as well as constitutional issues, began by determining whether section 215 could be interpreted to allow bulk collection of metadata by the government. The court stated "[t]he basic requirements for metadata collection under § 215, then, are simply that the records be *relevant* to an *authorized investigation* (other than a threat assessment)."[34] The problem with the government's methods of metadata collection, as argued by the appellants, was that it was not collecting evidence on a particular subject (an authorized investigation), but rather creating a huge pool of records that would later be relevant to a specific investigation.[35] The court then

28. *Id.* at 801.

29. *See id.*

30. U.S. CONST. amend. IV; *Clapper*, 785 F.3d at 801.

31. *Clapper*, 785 F.3d at 804.

32. *Id.* at 805.

33. *Id.* at 810.

34. *Id.* at 811.

35. *See id.*

concluded "the text of § 215 cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program."[36] The Second Circuit thus held that the telephone metadata program exceeded the power granted under section 215. The court acknowledged the "weighty" constit-utional issues brought up by the appellants regarding the telephone metadata program but did not reach them, having already held that the program was not authorized by section 215.[37] Though *Clapper* struck down the telephone metadata program, the Fourth Amendment issues it presents are too pertinent not to analyze.

This Comment's purpose is to analyze whether, under current Fourth Amendment jurisprudence, the telephone metadata program would be constitutional. Though this may seem like a moot exercise due to *Clapper's* holding, as well as the passage of the USA Freedom Act, which restricts the NSA from collecting telephone metadata in bulk,[38] the presence of other electronic surveillance programs still creates a need to analyze relevant Fourth Amendment issues pertaining to the telephone metadata program and other forms of mass surveillance.

II. SURVEILLANCE AND THE FOURTH AMENDMENT

A. Fourth Amendment and Exclusionary Rule Refresher

The ability for government agencies to access metadata, electronic communications, and conduct surveillance in general is governed by the Fourth Amendment. It states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[39]

36. *Id.* at 821.

37. *Id.* at 824.

38. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 (2015). This act restricts the production of tangible things (including telephone records) to the use of a "specific selection term." *Id.* This is used to parse through metadata collected by third parties. Individuals' metadata is still collectible and searchable, but the search is restricted. Erin Kelly, *Senate approves USA Freedom Act*, USA Today (June 2, 2015, 9:45 PM), http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/ [http://perma.cc/YWP3-CQLS].

39. U.S. CONST. amend. IV.

Note that the Fourth Amendment does not contain a remedy for unreasonable searches and seizures. When many people debate the federal government's ability to conduct mass surveillance, you may hear a proponent of civil liberties implore the surveillance supporter to "[u]se the Fourth Amendment!"[40] If the surveillance supporter followed the civil-liberty supporter's instructions and read the text of the Fourth Amendment word-for-word, the surveillance supporter might quip "Who cares about whether what the government did was illegal? The constitutional text does not actually penalize the government for illegal searches." What the civil liberties proponent should say is that the government's action is an illegal search, but that lacks the rhetorical beauty of crushing an opponent under the awe-striking power of the United States Constitution. The Supreme Court, long after the original thirteen states ratified the Bill of Rights, created a remedy for Fourth Amendment violations.

In *Weeks v. United States*,[41] the Supreme Court ensured that there would be an attention-grabbing consequence for illegal searches under the Fourth Amendment by creating the exclusionary rule, which excludes from trial any evidence obtained by violating the Fourth Amendment, regardless of whether the evidence shows a criminal defendant's guilt.[42] While *Weeks* was a dramatic change in Fourth Amendment jurisprudence, its exclusionary rule was not applied to the states until the Supreme Court decided *Mapp v. Ohio*[43] in 1961. After *Mapp*, evidence obtained through a Fourth Amendment violation could be excluded from criminal trials in either federal or state courts at the defense counsel's request.[44] With the Fourth Amendment text stated and the exclusionary rule reviewed, understanding the situations in which the exclusionary rule is applied will reveal whether the records produced through the telephone metadata program discussed in *Clapper* would be admissible as evidence against a defendant in a criminal trial.

B. Fourth Amendment Jurisprudence

Many Supreme Court cases address the Fourth Amendment and the exclusionary rule, so there are many cases which may help a federal court decide the constitutionality of a telephone metadata program or

40. *Fox News Primetime Republican Presidential Debate* (FOX News Channel television broadcast Aug. 6, 2015) (Senator Rand Paul used this phrase in the debate while discussing the NSA's bulk collection of phone records).

41. 232 U.S. 383 (1914).

42. *Id.* at 393. The exclusionary rule also excludes evidence obtained by violating the Fifth Amendment. *Id.*

43. 367 U.S. 643 (1961). *Mapp v. Ohio* incorporated the exclusionary rule to the states through the Fourteenth Amendment. *Id.* at 655.

44. *Id.*

other broad surveillance strategy. A few groups of cases will organize a complex web of Fourth Amendment jurisprudence into rules which are easier to apply to constitutional issues, like the telephone metadata program in *Clapper*, which would have been analyzed under the Fourth Amendment but for its ruling on statutory grounds.[45] Subpart (1) will outline when individuals have a legitimate expectation of privacy (without focusing on information gathered by or through devices meant to record or transmit communications), subpart (2) will delineate the third-party doctrine, and subpart (3) will explain the property-based approach to the Fourth Amendment.

1. The Legitimate Expectation of Privacy

a. Establishment of the Rule

Virtually all individuals expect privacy within their abodes and property, yet privacy interests do not necessarily end at one's property line or when homeowners cross the threshold of their front doors and expose themselves to public view. In *Katz v. United States*,[46] the Supreme Court held that "the Fourth Amendment protects people, not places."[47] Katz transmitted wagering information from Los Angeles to Miami and Boston by using a telephone booth.[48] Katz shut the telephone booth's door behind him when making the call to keep eavesdroppers at bay but his efforts were futile: the FBI heard Katz's end of the conversations by bugging the telephone booth with an electronic listening device.[49] Bugging telephone lines was constitutional before the Supreme Court decided *Katz* because surveillance without a physical trespass and without the seizure of tangible objects was not considered a search under the Fourth Amendment.[50] The Supreme Court discredited this view in *Katz*.

Justice Stewart, writing the majority opinion, stated that the FBI's actions were unconstitutional because "[o]ne who occupies [a phone booth], shuts the door behind him, and pays the toll . . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[51] Despite Justice Stewart writing the majority opinion, one of the most well-known rules of Fourth Amendment jurisprudence actually came from Justice Harlan's concurring opinion in *Katz*. He created a twofold requirement that must be met

45. *See* ACLU v. Clapper, 785 F.3d 787, 821 (2d Cir. 2015).

46. 389 U.S. 347 (1967).

47. *Id.* at 351.

48. *Id.* at 348.

49. *See id.* at 348, 352.

50. *Id.* at 353.

51. *Id.* at 352.

before Fourth Amendment protection extends to potential evidence: (1) "a person . . . exhibited an actual (subjective) expectation of privacy" and (2) "the expectation be one that society is prepared to recognize as 'reasonable.'"[52]

In *Katz*, the defendant shut the door behind him when making a call in the phone booth, which reveals that he actually expected his conversation would be private.[53] As for a legitimate expectation of privacy, the court determined that society considered Katz's expectation of privacy in the contents of his telephone conversation in a closed phone booth to be reasonable.[54] Since the second prong of the legitimate-expectation-of-privacy test assesses whether society deems the defendant's expectation of privacy reasonable, it is extremely malleable to a changing world and judicial creativity. It is the second prong that the ACLU relies on in *Clapper*,[55] as they would want federal courts to rule that society deems reasonable the expectation that the metadata generated by telephone calls is private and, therefore, protected by the Fourth Amendment's prohibition against unreason-able searches and seizures.[56] What is considered to be a legitimate expectation of privacy varies widely, with the unique facts of each case driving the legal conclusions.

b. When a Legitimate Expectation of Privacy Exists

Fourth Amendment issues exist in a variety of contexts, with household waste being no exception. *California v. Greenwood*[57] examined "whether the Fourth Amendment prohibits the warrantless search and seizure of garbage" left on a curb for collection by a local garbage company.[58] In *Greenwood*, police noticed vehicles would stop "during the late-night and early morning hours" for brief amounts of time at Greenwood's home.[59] Without seeking a warrant, police requested that the local trash collector pick up trash bags left on the curb in front of Greenwood's home and turn them over to the police.[60] Inside the bags were narcotics-related items, which convinced a judge to grant a warrant request to search the home, which contained cocaine and

52. *Id.* at 361 (Harlan, J., concurring).

53. *See id.* at 352. (majority opinion).

54. *See id.*

55. *See* ACLU v. Clapper, 785 F.3d 787, 821–25 (2d Cir. 2015).

56. U.S. CONST. amend. IV.

57. 486 U.S. 35 (1988).

58. *Id.* at 37.

59. *Id.*

60. *See id.* at 37–38.

hashish.[61] Greenwood argued that the search violated an expect-ation of privacy because the trash was in opaque plastic bags that would be mingled with others' trash and disposed of at the garbage dump, where linking the drug materials to particular suspects would be a near-impossible task.[62]

The Supreme Court disagreed. Justice White wrote in the majority opinion that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[63] Because Greenwood's garbage was exposed to innumerable third parties beyond his home's curtilage, the Supreme Court held that no Fourth Amendment protection extended to the garbage.[64] Concealing garbage in opaque bags and placing them in a publically-accessible location disavows Fourth Amendment protection, but hiding illegal substances behind high fencing in your yard would prevent the substances from being viewed by the general public. Fourth Amendment protection presumably applies through the legitimate-expectation-of-privacy test. So it would seem.

Fencing protects against street-level surveillance but allows a huge opening for sky-based surveillance. *California v. Ciraolo*[65] decided whether warrantless aerial observation from 1,000 feet of a fenced-in area of a backyard's curtilage violates the Fourth Amendment.[66] After receiving an anonymous tip that marijuana was growing in Ciraolo's backyard, the police found that a six-foot outer fence and ten-foot inner fence around the yard obstructed their street-level view.[67] Ever the creative bunch, the police procured a private plane, flew above the yard—in publically-navigable airspace—and photographed marijuana plants growing in the yard.[68] A judge issued a warrant, and officers subsequently seized marijuana at Ciraolo's home.[69] No sane person thinks they are at risk of surveillance from above by the state, so Ciraolo's case provided a chance for the Supreme Court to extend Fourth Amendment protection to fenced-in backyards. Not so.

61. *Id.* at 38.

62. *Id.* at 39.

63. *Id.* at 40.

64. *Id.* at 40–41.

65. 476 U.S. 207 (1986).

66. *Id.* at 209.

67. *Id.*

68. *Id.*

69. *Id.* at 209–10.

The Supreme Court equated aerial observation of a backyard to the neighborhood prowler watching you through a knothole in a fence, stating, "if there is an opening, the police may look."[70] Ciraolo countered that his yard was part of the curtilage of his home, preventing warrantless aerial surveillance.[71] Prior Supreme Court precedent defined a home's curtilage as "the area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life.'"[72] The Supreme Court accepted that Ciraolo's fenced-in yard and its crop were within the home's curtilage.[73] But despite occurring within the curtilage of a home, the Supreme Court found the warrantless observations did not violate the Fourth Amendment because the observations occurred in public airspace without physical intrusion.[74] Since private and commercial flight in public airways is routine, Ciraolo lacks a reasonable expectation that his marijuana plants would be constitutionally protected from naked-eye observation from 1,000 feet.[75] With even areas shrouded by a home's curtilage subject to warrantless surveillance, the police's natural next step was to subject activities within a home to warrantless surveillance from a public vantage point. This opportunity came at the turn of the millennium.

The story of *Kyllo v. United States*[76] starts out much like other Fourth Amendment cases: the police suspected Kyllo grew marijuana inside his home.[77] Unable to procure probable cause by viewing the home's exterior from a public road, the police used a thermal-imaging scanner to measure the amounts of heat within different parts of Kyllo's home.[78] The police discovered a relatively hot area near Kyllo's roof and sidewall as compared to neighboring homes.[79] Police secured a warrant with the temperature information and discovered an indoor marijuana-growth operation.[80] The Supreme Court found a boundary to police observations from publically accessible places by holding that thermal-imaging scans by devices not in general public use revealing details of

70. *Id.* at 210.

71. *Id.* at 212.

72. Oliver v. United States, 466 U.S. 170, 180 (1984) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

73. *Ciraolo*, 476 U.S. at 213.

74. *Id.*

75. *Id.* at 215.

76. 533 U.S. 27 (2001).

77. *Id.* at 29.

78. *Id.*

79. *Id.* at 30.

80. *Id.*

the home hidden but for physical intrusion were searches which require a warrant.[81] Justice Scalia, writing for the majority, clarified that the entire area within homes "is held safe from prying government eyes" and thus protected by the Fourth Amendment.[82] But "visual observation is no 'search'" according to Scalia.[83] What Scalia seems to say with these seemingly contradictory statements is that activities occuring within areas the human eyes could not see on their own are constitutionally protected. By adding the proviso "general public use" to devices that can detect activities occurring within homes, Scalia left a huge loophole open in his majority opinion future societal practices could exploit.[84] This proviso will be re-examined below in a new light, as it can be problematic with applications like Skype and Snapchat becoming prevalent in our society.[85] For now, two other categories must be explained.

2. The Third-Party Doctrine

The third-party doctrine is analogically similar to the assumption of risk affirmative defense in that an individual puts himself at risk of a calamity happening to him. A baseball fan smacked in the face by a broken bat flying through the air is just one example of a situation in which the assumption of risk affirmative defense would be used by a baseball team defending itself from a tort suit. In the Fourth Amendment context, the "calamity" which could befall an individual is for their information, freely-given under an apparent aura of confidentiality to a third party, is disclosed to the government, which then initiates a criminal prosecution based on the information gathered. In *Smith v. Maryland*,[86] the Supreme Court affirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[87] *Smith's* facts are crucial, as the device used to

81. *Id.* at 40.

82. *Id.* at 37. Kyllo, thus, had a reasonable expectation of privacy in the heat output of his drug-growing lamps. *Id.* at 34. Admittedly, Kyllo is a tough case to classify in my three categories of Fourth Amendment jurisprudence relating to mass surveillance (those being (1) the legitimate expectation of privacy; (2) the third-party doctrine; and (3) the property-based approach to the Fourth Amendment), as it foreshadows Scalia's reintroduction of the property-based approach. *See, e.g.*, Jones v. United States, 132 S. Ct. 945, 949 (2012). However, I decided that Kyllo was best suited for the legitimate expectation of privacy category because it highlights one of the few reasonable expectations of privacy that is considered a bright-line rule. *See Kyllo*, 533 U.S. at 40.

83. *Kyllo*, 533 U.S. at 32.

84. *See id.* at 34.

85. *See infra* Part V(B).

86. 442 U.S. 735 (1979).

87. *Id.* at 743–44.

gather the voluntarily-disclosed information in *Smith* works similarly to the telephone metadata program in *Clapper*.[88]

Smith robbed a woman in Baltimore, but he was not identified by her initially.[89] She then received threatening and obscene phone calls from the robber who once asked her to step outside, and at that time, she saw a 1975 Monte Carlo pass her home.[90] The police later spotted the same car and used its license plate number to identify a suspect, Smith.[91] To confirm that he was the source of the woman's annoying phone calls, a telephone company installed a pen register—without a warrant—to record the numbers dialed from Smith's home.[92] Smith turned out to be the caller as well as the robber, and he was arrested.[93] A notable fact is that Smith used his home telephone to make his calls, yet the Supreme Court determined that his conduct failed to preserve the privacy of the numbers he dialed because he voluntarily provided the telephone company with the numbers needed to complete his call.[94] Similar outcomes have occurred in other contexts.

Miller, a man suspected of operating an unregistered still, had accounts with two banks in Georgia.[95] Previously, a warehouse rented to Miller caught fire, and the authorities found distillery paraphernalia in it.[96] A grand jury issued subpoenas to the presidents of the two banks to produce all records of accounts in the name of Mr. Mitch Miller over a span of several months.[97] The presidents complied.[98] Miller's case traveled all the way to the Supreme Court, which held that he had no protected Fourth Amendment interest in the disclosure of the bank records of his accounts.[99] The Supreme Court determined that the account records belonged to the banks, not to Miller, and that the

88. *Compare id.* at 741 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)) ("These devices do not hear sound. They disclose only the telephone numbers that have been dialed."), *with* ACLU v. Clapper, 785 F.3d 787, 793 (2d Cir. 2015) ("[T]elephone metadata do not include the voice content of telephone conversations. Rather, they include details about telephone calls.").

89. *Smith*, 442 U.S. at 737.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* at 743.

95. United States v. Miller, 425 U.S. 435, 437 (1976).

96. *Id.*

97. *Id.* at 437–38.

98. *Id.* at 438.

99. *Id.* at 440.

information in the records was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[100] Despite the fact that Miller likely assumed that the information about his bank accounts was confidential and to be used for a limited purpose, the Fourth Amendment was held to not prohibit the government from obtaining the records.[101] While records created from bank transactions and dialed phone numbers are not protected by the Fourth Amendment, an even more critical issue for understanding the limits of mass surveillance is whether the content of conversations entirely held within a home or hotel room receive constitutional protection.

Nashville was the site of a trial in which Jimmy Hoffa was convicted for trying to bribe members of a jury in a separate case, in which he allegedly violated a section of the Taft-Hartley Act.[102] During this previous case, known as Test Fleet, a man named Edward Partin accompanied Hoffa and his cohorts in a hotel suite, hotel lobby, courthouse, and other areas around Nashville.[103] Partin served as a government informant as he stayed near Hoffa.[104] Partin provided crucial information about Hoffa and his associates' desire to bribe the Test Fleet jury members.[105] Partin received access to Hoffa's hotel suite, and by doing so, obtained verbal evidence against Hoffa's interest.[106] Hoffa argued that Partin's failure to reveal his role as an informer destroyed the permission Hoffa gave for Partin to enter Hoffa's hotel suite and constituted an illegal search.[107] Nevertheless, Hoffa's argument failed.

Hoffa's legal team implicated no interests protected by the Fourth Amendment: "[Hoffa] was not relying on the security of the hotel room; he was relying upon his misplaced confidence that Partin would not reveal his wrongdoing."[108] The Supreme Court additionally noted that Hoffa invited Partin into the hotel room and incriminated himself either directly to Partin or within Partin's presence.[109] *United States v. White*[110] and *Lopez v. United States*[111] came to a similar conclusion: the

100. *Id.* at 440, 442.

101. *See id.* at 443.

102. Hoffa v. United States, 385 U.S. 293, 294–95 (1966).

103. *Id.* at 296.

104. *Id.* at 299.

105. *Id.* at 296.

106. *See id.* at 302.

107. *Id.* at 300.

108. *Id.* at 302.

109. *Id.*

110. 401 U.S. 745 (1971).

111. 373 U.S. 427 (1963).

government need not procure a warrant when a government agent, unknown to a defendant, hides electronic equipment on his person to record the defendant's words and then offers those words as evidence.[112] The Supreme Court summarized the dangers of conversing about criminal activities with others by stating:

> Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.[113]

The sum of the third-party doctrine is this: any information voluntarily provided to others is not subject to Fourth Amendment protection, no matter whether the information is exchanged in the public square or within the sanctity of a home.

3. The Property-Based Approach to the Fourth Amendment

The property-based approach to the Fourth Amendment seemingly disappeared in *Katz*.[114] Justice Scalia held differently in *Jones v. United States*.[115] In *Jones*, police attached a GPS tracker to the undercarriage of Jones' Jeep while it was parked in a public lot.[116] The GPS locational data showed that Jones frequented a stash house containing cash, cocaine, and cocaine base.[117] Scalia determined that attaching the GPS to the Jeep constituted a search per the meaning of the Fourth Amendment at its adoption.[118] Scalia made this confident assertion by stating that a car is an "'effect' as that term is used in the [Fourth] Amendment."[119] A distinguishing factor in this case is that Jones owned the Jeep before the government installed the GPS device on its undercarriage.[120] This is different than police officers inserting a beeper

112. *White*, 401 U.S. at 749; *Lopez*, 373 U.S. at 438–440.

113. *White*, 401 U.S. at 752.

114. Katz v. United States, 389 U.S. 347, 353 (1967).

115. 132 S. Ct. 945 (2012).

116. *Id.* at 948.

117. *Id.* at 948–49.

118. *Id.* at 949.

119. *Id. See* U.S. CONST. amend. IV; United States v. Chadwick, 433 U.S. 1, 12 (1977) ("It is true that . . . automobiles are 'effects' under the Fourth Amendment, and searches and seizures of automobiles are therefore subject to the constitutional standard of reasonableness.").

120. *Cf. Jones*, 132 S. Ct. at 952 (distinguishing the facts of Jones' case from two cases that the Government relied upon to argue that what happened was not a search).

(locational transmitter) into a container before defendants purchase the containers, as that action, which monitored the public vehicular movements of the suspects, was not a search.[121] With Justice Scalia resurrecting the property-based approach to the Fourth Amendment in *Jones*, the relevance of the legitimate-expectation-of-privacy test came into question.

Justice Scalia helped clarify the importance of the *Katz* analysis in light of his majority opinion in *Jones* by saying, "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."[122] The implication of this statement for Fourth Amendment issues involving mass surveillance is substantial and will be further analyzed below.[123] Justice Scalia's property-based approach to the Fourth Amendment continued to evolve as he further opined on the matter in 2014.

Florida v. Jardines[124] determined whether a drug-sniffing dog used on a homeowner's porch to sniff for contents within the home constitutes a search under the Fourth Amendment.[125] An anonymous tipster informed police that Jardines had marijuana in his home.[126] Police noted no activity occurring around the home and decided to walk to the front door—with a drug-sniffing dog.[127] The dog indicated that it smelled marijuana in the home, and this was enough information for a judge to issue a warrant, leading to officers finding marijuana.[128] The Supreme Court held that because the dog revealed information which was within a home, its action was a search under the Fourth Amendment.[129] Justice Scalia opined why the officers' conduct was so inappropriate relative to implicit neighborhood customs.

> This implicit license typically permits the visitor to approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave. Complying with the terms of that traditional invitation does not

121. *See* United States v. Knotts, 460 U.S. 276 (1983) (holding that the public movements of a suspect on roadways was not a search under Fourth Amendment).

122. *Jones*, 132 S. Ct. at 953 (emphasis removed).

123. *See infra* Part V(A).

124. 133 S. Ct. 1409 (2013).

125. *Id.* at 1413–14.

126. *Id.* at 1413.

127. *Id.*

128. *Id.*

129. *See id.* at 1417–18 (holding that the officers and the dog were on a Constitutionally protected area of the defendant's home and thus there was an intrusion).

> require fine-grained legal knowledge; it is generally managed without incident by the Nation's Girl Scouts and trick-or-treaters.[130]

In contrast to the practices of door-to-door cookie sellers and Halloween candy seekers, police officers walking a dog close enough to a home to discover incriminating evidence without a warrant offended Justice Scalia's view of how people conduct themselves regarding the property of others.[131] The outcome of *Jardines* is very similar to *Kyllo* in that Justice Scalia thought that it was not a generally accepted practice to thermally scan a person's home to reveal activities occurring behind the home's front door and walls.[132]

Besides labeling dog sniffs occurring on a home's front porch and GPS devices attached to vehicles as Fourth Amendment searches, the Supreme Court also addressed whether tracking devices attached to people, without consent, constitute a search. Though *Grady v. North Carolina*[133] did not determine the constitutionality of a sex-offender tracking program wholesale, it did declare that "[North Carolina]'s program is plainly designed to obtain information. And since it does so by physically intruding on a subject's body, it effects a Fourth Amendment search."[134]

With the Fourth Amendment jurisprudence refresher completed, the necessary ingredients exist to decide whether the telephone metadata program featured in *Clapper* violates the Fourth Amendment.

III. CLAPPER'S CONSTITUTIONAL CLAIM OUTCOME

The telephone metadata program in *Clapper* is constitutional because it falls under the third-party doctrine of Fourth Amendment jurisprudence. The telephone metadata program in *Clapper* works similarly to the pen register technology (capable of recording telephone numbers dialed) featured in *Smith v. Maryland*.[135] The telephone metadata program in *Clapper* required Verizon to produce call records daily of all calls made through its system where one or both ends of the call

130. *Id.* at 1415.

131. *Id.* at 1416.

132. Kyllo v. United States, 533 U.S. 27, 34 (2001). Shades of Justice Scalia's "general public use" proviso seem present in *Jardines*. *Jardines*, 133 S. Ct. at 1415.

133. 135 S. Ct. 1368 (2015) (per curiam).

134. *Id.* at 1371.

135. 442 U.S. 735, 737 (1979) (explaining that a pen register records the numbers a person dials on their telephone in their home).

were within the United States.[136] The ACLU may argue that the telephone metadata program's systemic, nationwide reach distinguishes it from the holding in *Maryland v. Smith v. Maryland*. This argument will likely fail because, while the number of people whose metadata is collected is far greater in *Clapper*,[137] the legal principle undergirding both *Clapper* and *Smith v. Maryland* is the same: a person has no legitimate expectation of privacy in information voluntarily turned over to third parties.[138]

The ACLU could also argue that the telephone metadata program in *Clapper* differs from *Smith v. Maryland* because the telephone metadata program did not require physically installing pen registers for all Verizon account holders. This argument falls flat. There was no physical system needed to produce bank account records in *United States v. Miller*,[139] but that did not stop the Supreme Court from ruling that bank account records were disclosable without a warrant.[140] *Smith* and *Miller* speak to the proposition that when individuals perform activities that generate data points or willingly provide content to third parties, those third parties may then disclose that information to the government, and the government need not seek a warrant when obtaining records from a third-party source.

The legal conclusion in this section is surely disturbing to many individuals. However, it is the correct conclusion, as it follows the third-party doctrine. Not surprisingly, some have called for the revision of the third-party doctrine as a means of reducing the danger of dragnet-style government mass surveillance. These calls have come even from the Supreme Court.

IV. CALLS FOR REFORM

Many different sources have called for reform of Fourth Amendment jurisprudence. This section will feature three of those sources: (A) Justices of the Supreme Court; (B) legal academics; and (C) my proposed jurisprudential reform, which will protect individuals from some forms of government mass surveillance by preventing the government from accessing the content of individuals' conversations directly, at least without seeking the consent of one of the parties who participated in the conversation. I call this the derivative-consent doctrine; just because parties consent to converse with each other does not allow the government to listen in to (or watch, if referring to a

136. ACLU v. Clapper, 785 F.3d 787, 795–96 (2d Cir. 2015).

137. *See id.* at 796.

138. *Smith*, 442 U.S. at 743–44.

139. 425 U.S. 435 (1976).

140. *Id.* at 442.

videophone conversation through an application such as Skype) the conversation as if a party also consented to that.

A. Calls for Reform from the Supreme Court

Some Justices of the Supreme Court have pondered the need for jurisprudential reform due to the increasingly electronic and non-physical nature of surveillance techniques. Justice Sotomayor noted that "the Government will be capable of duplicating the monitoring undertaken in this case [*Jones*] by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones."[141] She further stated that the property-based approach to the Fourth Amendment is not as useful when dealing with electronic surveillance not dependent on physical encroachments on property.[142] After discrediting Justice Scalia's approach in *Jones*, Justice Sotomayor reviewed the dangers of the third-party doctrine, as in today's digital age people reveal large quantities of information to third-parties.[143]

The amount of information third parties receive about our goings-on is dramatic. Justice Sotomayor further wrote that people "disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[144] But despite individuals' willingness to conduct their lives in a manner which third parties may observe, Justice Sotomayor acknowledged that people likely "would [not] accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."[145] One solution the Supreme Court may implement in the future is to assert that individuals have a legitimate expectation of privacy in the information they exchange to third parties in the course of conducting their daily internet surfing, calls or texts, e-mail addresses, and online purchase orders.[146]

Justice Alito also wrote a concurrence in *Jones*. His solutions to the difficult Fourth Amendment problems created by electronic means of

141. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

142. *Id.*

143. *Id.* at 954–57.

144. *Id.* at 957.

145. *Id.*

146. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (detailing the traditional legitimate-expectation-of-privacy test regarding third parties). Justice Scalia acknowledged that *Katz* would apply to "the transmission of electronic signals without trespass." *Jones*, 132 S. Ct. at 953. As society evolves, so will our privacy expectations. *Id.* at 955 (Sotomayor, J., concurring).

surveillance are not through case law but through the political branches.[147] Justice Alito highlighted wiretapping as an example of a difficult Fourth Amendment issue that was reformed through legislation instead of case law.[148] Justice Alito explained why he believes the proper solution to electronic surveillance reform is found in Congress, stating that a "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[149]

Justice Sotomayor's concurrence suggests the need for a jurisprudential reform to change the third-party doctrine, seemingly based on *Katz's* legitimate-expectation-of-privacy test, which is designed to measure society's perception of when Fourth Amendment protection exists.[150] Justice Alito's concurrence supports a legislative reform to the electronic surveillance issue. The best solution may require a bit of both.

B. Academic Perspectives

1. Hosein and Palow Article

A symposium article by Gus Hosein & Caroline Wilson Palow addresses some of the Fourth Amendment issues created by the many technological marvels that we take for granted.[151] The pervasiveness of modern communications technology in our society is well-known. Those who choose not to use such technology "would be socially and economyically" excluded.[152] Technologies requiring remote access are well suited for the reasonable expectation of privacy standard to be applied to them.[153] The cameras and microphones incorporated in many devices we carry present the danger for incredible intrusions into our conversations, even potentially providing unwanted glances into our homes. Hosein and Palow discuss how cameras and microphones in computers "under the control of an offensive technology, could record . . . information about the computer's surroundings, from private conversations to pictures and video of the objects and persons who happen to be in front of the camera."[154] After outlining the danger that

147. *Jones*, 132 S. Ct. at 962–63 (Alito, J., concurring).

148. *Id.*

149. *Id.* at 964.

150. *Katz*, 389 U.S. at 361; *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

151. Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071 (2013).

152. *Id.* at 1077.

153. *Id.* at 1093.

154. *Id.* at 1094.

microphone- and camera-equipped technology presents, Hosein and Palow offer a solution:

> If, while the computer resides in such a protective place, the government could not gain access to it without a warrant, then the government should not be able to install an offensive technology on that device merely because, for some fractional amount of time, it may be located outside of the protected sphere.[155]

Working off Hosein and Palow's proposed jurisprudential solution, consider this possibility. A law student, eyes glazing over from completing her law school writing requirement on her computer in her apartment, decides to walk down the street to get a much-needed caffeinated beverage at her favorite coffee shop. It contains a publically accessible internet network, and she figures she can continue writing her paper while sipping her drink. Unbeknownst to her, a fellow law student discovered that she had a strong interest in illegal horticulture and disclosed this information to the government. An agent, waiting for her to leave the protected area of her apartment, followed her to the coffee shop, where he used the publically accessible internet network to secretly upload malware to her computer.

When the law student returns to her apartment, she places her computer in the same room as her special "plants" with the computer's camera facing the plants. After she retires for a well-deserved rest, the malware within her computer activates, serendipitously using her computer's camera to record images of the marijuana growing in her room. The images provide sufficient probable cause for a judge to grant a warrant, and she is arrested for her illegal marijuana growing. The danger Hosein and Palow warn of is the ability of a webcam to show the government images that it would not be able to, absent physical invasion of a person's abode. Their article states that warrants must be issued for the type of situation encountered by our illegally-gardening law student.[156]

Another issue involves the information that can be gathered from cell phones. International Mobile Subscriber Identity (IMSI) catchers impersonate mobile base stations, allowing mobile phones to be located and identified within range of the device.[157] Although IMSI catchers can intercept content transmitted by mobile phones, Hosein and Palow

155. *Id.* at 1095–96 (citation omitted).

156. *See id.* at 1096 ("[A] person has a reasonable expectation of privacy in the contents of her computer, and in its ability to transmit audio, video, or locational information regarding her surroundings when those surroundings are likely to constitute traditionally protected areas such as the home and the office.").

157. *Id.* at 1097.

state that the content is protected by the Wiretap Act, forcing police to obtain a warrant prior to examining the content of communications.[158] Another restriction on tracking individuals' whereabouts through cell phones is if they enter their homes. The Supreme Court, in *United States v. Karo*,[159] did not allow a tracking device (or beeper) implanted in a drum of drug-making ingredients to show the precise location—within Karo's home—where the drum sat without a warrant.[160] Similarly, if an IMSI catcher indicated a cell phone's location within a person's home, that information would not be collectible unless the police obtained a warrant.[161] Hosein and Palow's analysis shows that it is possible that courts will restrict the ability of the government to track a person's whereabouts at all times through IMSI catchers, while also arguing that the government could not install malware on a computer in a public place, and then activate the malware as it sits in a constitutionally-protected location, such as a person's abode.

2. Harvard Law Review's Proposed Jurisprudential Solution for Mass Surveillance

The Harvard Law Review shares the concerns that many others in our society have concerning mass surveillance. The esteemed scholarly publication especially worries that "when the focus of surveillance turns from monitoring a specific place to monitoring a specific person, the potential for uncovering the intimate details of that person's life is substantially higher."[162] As a solution to preventing the government from gathering too much intimate information on an individual, Harvard Law Review proposes a two-factor test to determine whether enhanced observation is a search: (1) the intensity of the surveillance and (2) the state's ability to synthesize the information collected to produce a particularized profile of an individual.[163]

The reasoning behind this test is "to mirror the practical barriers that once constrained police conduct."[164] Additionally, the test counters the third-party doctrine because "economic considerations no longer

158. *Id.*

159. 468 U.S. 705 (1984).

160. *Id.* at 716.

161. Hosein & Palow, *supra* note 151, at 1098–99.

162. Recent Case, *Seventh Circuit Holds That GPS Tracking Is Not a Search – United States v. Garcia, 474 F.3d 994 (7th Cir. 2007), reh'g and suggestion for reh'g en banc denied, No. 06-2741, 2007 U.S. App. LEXIS 8397 (7th Cir. Mar. 29, 2007)*, 120 HARV. L. REV. 2230, 2235 (2007).

163. *Id.*

164. *Id.* at 2236.

stand as a barrier to widespread, intrusive observation."[165] While the rule proposed by the Harvard Law Review is normative, it at least recognizes the widespread danger caused by mass surveillance. But it is too difficult to measure. What one judge may consider to be soft surveillance may to another be overly intrusive. There is a better solution.

3. How Electronic Information is Captured and a Property-Based Solution

There are other surveillance programs in operation besides the telephone metadata program highlighted in *Clapper*. One example is PRISM, a program that collects the contents of communications and other assorted information through internet-based service providers such as Google, Apple, and Facebook.[166] The NSA, using PRISM, can access "email, chat, photos, stored data, voice over IP, and other information stored on participating companies' servers."[167] Another surveillance method is called upstream collection, which means that the government collected communications passing through a telecommunication provider before they reached their destination.[168]

If PRISM and upstream collection were not enough, another option is XKeyscore, which allows analysts to search metadata, the content of e-mails, and internet browser history, without even knowing the e-mail address of the person targeted by the search.[169] Other information discoverable with XKeyscore includes social media activity and browsing data.[170] With an array of surveillance programs at the government's disposal, there may be little hope of keeping any electronic communications truly private.

Under *Smith v. Maryland*,[171] it may be argued that any communications or data passed through an internet service provider does not constitute a search.[172] One way to preclude this outcome is to pass legislation vesting property rights in electronic communications and

165. *Id.* at 2237.

166. Megan Blass, Note, *The New Data Marketplace: Protecting Personal Data, Electronic Communications, and Individual Privacy in the Age of Mass Surveillance Through a Return to a Property-Based Approach to the Fourth Amendment*, 42 HASTINGS CONST. L.Q. 577, 579–80 (2015).

167. *Id.* at 580.

168. *Id.* The NSA established a room at AT&T's Folsom Street Facility in San Francisco to collect all communications passing through. *Id.*

169. *Id.* at 581.

170. *Id.*

171. 442 U.S. 735 (1979).

172. Blass, *supra* note 166, at 586.

personal information.[173] Doing so would apply Justice Scalia's property-based approach to the Fourth Amendment as exhibited in *Jones*.[174] Bypassing a firewall or password protection to access content would be construed as a Fourth Amendment search if electronic comm-unications were considered property, as is stated in this proposal.[175] But this proposal could be problematic as well because it could chill work-place communications by scaring people from sending e-mails to sources that the original writer did not explicitly consent could receive such information.

C. Author's Proposal: Derivative-Consent Doctrine

I agree that reform is needed in the Fourth Amendment's jurisprudence to protect individuals from mass surveillance capabilities. But the trick is in balancing the need to protect civil liberties with the need to secure the United States from threats, particularly those originating from overseas. I disagree with the notion that the third-party doctrine must be eliminated. Information voluntarily disclosed to others should be, in most cases, available for anyone to view, including the government, without consequence.[176] There are, however, some situations in which individuals did not turn over or create information voluntarily, but the government then decides to peruse the communi-cation anyway.

The derivative-consent doctrine is designed to prevent the government from accessing the content of conversations, as well as controlling or using devices, without another individual first revealing the information or operating a device. The derivative-consent doctrine is best thought of as an alternative approach to the *Katz* legitimate-expectation-of-privacy test[177] and is not designed to eviscerate current Fourth Amendment jurisprudence. What the derivative-consent doctrine is designed to do is prevent Orwellian-style mass surveillance from becoming a fixture in the United States.

---

173. *Id.*

174. *Id.*; United States v. Jones, 132 S. Ct. 945, 949 (2012).

175. Blass, *supra* note 166, at 594.

176. Smith, 442 U.S. at 743–44. Note that the Smith opinion emphasizes the word "voluntarily" when referring to information given to third parties. *Id.*

177. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). While I value the Katz legitimate-expectation-of-privacy test for its ability to assert Fourth Amendment rights based on how society changes, the test appears too vulnerable to differing outcomes based on political philosophy and ideological alliances. I believe a consent-based test is not as vulnerable to the changes in the ideological composition of the Supreme Court and general populace, and desire it to provide a baseline of protection against Orwellian mass surveillance no matter what part of the political spectrum controls surveillance efforts at a certain time.

Explaining the derivative-consent doctrine is best done through examples, though I will attempt to state it as a legal rule. Consent in the context of surveillance is best thought of as two levels. Level one is an individual's voluntary assertion of consent. For instance, when a person dials a number or sends a text message that person voluntarily consents to the cell-phone provider recording the numbers, the length of the text or call, and other information pertinent for billing purposes. Surveillance performed at level one, in which individuals create meta-data through their need to exchange information with a service provider in order for a device to perform a specified task, is constitutional under *Smith* and the third-party doctrine.[178]

Level two is where Orwellian surveillance efforts go to die. Level two surveillance occurs when a provider discloses the contents of electronic messages to the government and when a device owned by an individual is hijacked by others (most likely through malicious software), allowing it to reveal information that otherwise would not have been seen or heard. Level two surveillance is explicitly outside of the third-party doctrine because information gathered through it is not voluntarily provided by the person the government is investigating.[179] Gathering information using means beyond a person's voluntary acts, therefore, requires a warrant for such an act constitutes a search under the Fourth Amendment.

V. DERIVATIVE-CONSENT DOCTRINE IN ACTION

Because the derivative-consent doctrine is more difficult to understand when stated abstractly, I will use several examples to show the application of the doctrine. Not all of these examples will resolve themselves using the derivative-consent doctrine. Some examples demonstrate that the derivative-consent doctrine is not meant to displace existing Fourth Amendment jurisprudence. For instance, the first example comes straight out of *Jones*.

A. The Phantom Activation of a Stolen Vehicle Detection System

Justice Alito's concurrence in *Jones* proposed a hypothetical which, he insinuated, may conflict with Justice Scalia's property-based approach to the Fourth Amendment. For purposes of this example, equate a vehicle's built-in GPS navigation system with a stolen vehicle

178. *See* Smith, 442 U.S. at 743–44.

179. *Id.* "This Court consistently has held that a person has no legitimate expectation of privacy in information he *voluntarily* turns over to third parties." *Id.* (emphasis added). But note that the third-party doctrine does not require warrants to track the public movements of individuals. *Id. See* United States v. Knotts, 460 U.S. 276 (1983) (holding that the public movements of a suspect on roadways was not a search under Fourth Amendment).

detection system. Justice Scalia, in his majority opinion in *Jones*, wrote "suppose that the officers in the present case [*Jones*] had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased. Would sending of a radio signal to activate this system constitute a trespass to chattels?"[180] Justice Scalia, in his majority opinion, also mentioned in dicta that this type of situation may not be a trespass, since the system was activated with a signal.[181] While it is difficult to tell how Justice Scalia would answer this question, this is an example of a scenario answerable by either the derivative-consent doctrine or by Justice Scalia's property-based approach to the Fourth Amendment.

The derivative-consent analysis works like this. When the car was on the dealer's lot, it belonged to the dealer.[182] At this time, the dealer could consent to the government activating the stolen-vehicle detector within the car, should it be stolen while the dealer controls the car. Once the dealer sells the car, the ability to use its stolen vehicle detector lies with the new owner. Suppose the owner's spouse takes the car for a spin without telling the owner, and the owner assumes it stolen. The owner then activates the car's stolen vehicle system, and finds that the car is at the local supermarket (the spouse took it on a grocery run). Information created by the voluntary use of the system by the car's owner may be turned over to the government without a warrant. This is level one surveillance.

To upgrade the surveillance at issue to level two, suppose that, as in *Jones*, police track the movements of a suspect. However, instead of attaching a physical GPS unit to the vehicle's undercarriage,[183] officers instead tracked the device by remotely activating the system, as Justice Alito's hypothetical states.[184] This is level two surveillance, and thus constitutes a search under the Fourth Amendment, because the system was not active due to the voluntary consent of its owner.

Alternatively, Justice Alito's hypothetical can be answered using Justice Scalia's property-based approach to the Fourth Amendment. Once the car (and thus the components within the car, including the stolen vehicle detection system) is purchased, it is the owner's property. If the stolen vehicle detection system is remotely activated by someone other than the owner, this would also be a search that requires a

180. United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).

181. Jones, 132 S. Ct. at 953 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis.") (emphasis removed).

182. Whether the car belonged to the dealer or to the car company that made it is irrelevant to the analysis because the outcome is the same.

183. Jones, 132 S. Ct. at 948.

184. *Id.* at 962 (Alito, J., concurring).

warrant, because the car (including its inner components) is an "effect" under the Fourth Amendment.[185] Hijacking someone else's property for your own use, without a warrant, should be impermissible under the Fourth Amendment.

B. The Skype Friend Becomes an Enemy

Skype provides a whole new world of communication possibilities. It is the darling of couples in long-distance relationships who seek more than to hear the voice of their loving companion, as it uses cameras incorporated within computers to show a person's face on the other end of the call. Besides showing the person on the other end of the call, the image on your computer is likely to show what is immediately behind the person too. Besides warming the hearts of long-distance lovers, Skype video calls create interesting Fourth Amendment issues.

Assume that a Skype caller observes a suspicious-looking plant behind the person on the other end of the call. The background image of the call indicates that the person on the other end of the call is within his home. After completing the call, the law-and-order minded friend calls police and reports that her friend has marijuana in his bedroom, located at address X. Police rely on the information voluntarily provided to them by seeking and receiving a search warrant. Police then successfully discover marijuana at the address and arrest the boy who was on the other end of the call.

Unlike the previous example, the derivative-consent doctrine does not apply. The answer to this Fourth Amendment issue is an easy one: because the boy trusted that the girl he called would not give away the fact that he had a marijuana plant in his bedroom, the information she provided receives no Fourth Amendment protection, as it is subject to the third-party doctrine.[186]

C. E-mail and Social-Media Messages

The next example depicts whether the content of e-mail and social-media messages may be disclosed to the government without a warrant. Before jumping into the analysis, a proviso is required. A social-media message's contents are defined as only intended for individuals designated as receivers; they are not pronouncements for the whole world to know about. E-mails and social-media messages may appear to be subject to the third-party doctrine because they are processed through an internet-service provider.[187] However, the derivative-consent doctrine provides a different outcome.

185. U.S. CONST. amend. IV.

186. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

187. *See* Blass, *supra* note 166, at 586 ("*Smith* made it such that surveillance and investigation involving collection or review of communications or data that have passed through an internet service provider, a precondition satisfied anytime the internet is involved, do not constitute searches.").

A person sends an e-mail from his apartment, which has a private connection to the internet. The e-mail contains metadata, most notably the e-mail addresses of the sender and the receiver. The metadata may be disclosed by the internet-service provider because it is only level one surveillance. The sender consents to the internet-service provider using the e-mail addresses provided to send the message. This is obvious because the sender would not send the message if he did not consent to allowing the service provider to use the most basic information required in transmitting the message. Now suppose that the provider, instead of merely transmitting the message, decides to disclose its content to the government. This is level two surveillance, and constitutes a search under the Fourth Amendment. Unless the sender consents that the provider also show the government the contents of the message, such a disclosure requires a warrant.

Even without arguing that e-mails should be considered personal property,[188] other constitutional jurisprudence dictates Fourth Amendment protection for messages or packages sent through mailing services.[189] Letters and other sealed packages are "effects" under the Fourth Amendment, meaning "warrantless searches of . . . effects are presumptively unreasonable."[190] *United States v. Jacobsen*[191] featured a damaged package that was opened by a third-party carrier.[192] The carrier and DEA agents determined that the package contained cocaine.[193] The Supreme Court held that the package did have Fourth Amendment protection, but lost such protection because a third-party opened the package, albeit because it was accidentally damaged by a forklift.[194]

When individuals send letters, they expect those letters to remain private.[195] It is illogical to conclude that messages sent through e-mail or through a social-media message would receive different treatment than that of physical letters and packages sent through mailing services. Moreover, e-mails, messages, and attached files are not damageable in "shipping" the same way that physical letters and packages are, so

188. *Id.* at 586. If emails are designated as personal property, they would likely be considered an "effect" under the Fourth Amendment. U.S. CONST. amend. IV.

189. I define "mailing services" as the Postal Service, UPS, FedEx, W.B. Mason, and other similar parcel shipping and delivery services.

190. United States v. Jacobsen, 466 U.S. 109, 114 (1984).

191. 466 U.S. 109 (1984).

192. *Id.* at 111.

193. *Id.* at 111–12

194. *Id.* at 111, 115.

195. *Id.* at 115.

internet-service providers will not have the excuse that they opened the e-mail in order to transfer it to an unbroken container.

The *Katz* analysis on its own may provide protection by analogizing physical letters and packages to e-mails, messages, and attachments.[196] But the derivative-consent doctrine provides protection that is not based on society's perception of what privacy is,[197] so it would be best to hold that under it, e-mails and social-media messages are not disclosable to the government without a warrant, unless the sender or the receiver consents that the internet-service provider also send the message to the government.

While the derivative-consent doctrine reduces the voluntary power of third-party internet-service providers serving as information transmitters to disclose information to the government, it more import-antly prevents Orwellian-style surveillance of the contents of electronic communications. No nation with an amendment protecting against "unreasonable searches and seizures" shall force its citizens into a shell of secrecy.[198] Doing so will harm our ability to conduct business, make friends, seek our soul mates, and conduct our lives without feeling like a shadow of surveillance falls over our every communication.

CONCLUSION

This Comment began by comprehensively reviewing the facts of *ACLU v. Clapper*. It then reviewed the text of the Fourth Amendment, as well as the Supreme Court's remedy for violations of the Fourth Amendment, the exclusionary rule. What followed was an outline of three categories of Fourth Amendment cases: (1) cases concerning the legitimate expectation of privacy; (2) the third-party doctrine; and (3) the property-based approach to the Fourth Amendment. After determining that the outcome of the Fourth Amendment claim in *Clapper* would have been an assertion of the third-party doctrine as a justification for Verizon's telephone metadata program, the Comment considered several solutions.

Justice Sotomayor proposed that the third-party doctrine be revised because the metadata produced by mundane daily tasks is so great that individuals' intimate associations may be revealed. She also argued that American citizens likely would have an expectation of privacy in the data their electronic interactions create. Justice Alito argued that a better solution for restricting mass surveillance would be to enact legislation restricting practices, such as the remotely activating theft-detection systems in vehicles, which could conceivably be used to track a person's movements at all times.

196. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

197. *Id.*

198. U.S. CONST. amend. IV.

Besides the Supreme Court, a few solutions to the metadata issue were highlighted from other academic sources. Making sure that malware uploaded surreptitiously to individuals' computers in public networks could not be used to turn on a computers' microphone and camera was the focus of one source, as was the ability of ICMI catchers to constitutionally detect individuals' public movements. Another source, such as the Harvard Law Review, created a two-factor test for surveillance, but I found the test easy to manipulate based on whether a judge has a civil libertarian or a law and order bent. Still one other source advocated that Congress should vest property rights in electronic communications. None of these sources provided a comprehensive solution.

I proposed what should provide an adequate balance between civil liberties and security. My derivative-consent doctrine divides surveillance into two levels. Level one surveillance involves information created by an individual's voluntary assertion. This includes metadata, the information that individuals consent to provide to telecommun-ications companies or mail carriers in order to send messages to the intended recipients. Level one surveillance is constitutional under the third-party doctrine and does not require a warrant to procure.

Level two surveillance constitutes a search under the Fourth Amendment. The contents of e-mails, social-media messages, as well as any information gathered about a person that he did not volunteer to provide is included in level two surveillance. Despite the derivative-consent doctrine's invention, it does not displace existing Fourth Amendment jurisprudence. What the derivative-consent doctrine does do is provide a supplementary method for thinking through mass surveillance issues that prevents the government from ever asserting an Orwellian-style surveillance system over the United States.

An example of the overlap between the derivative-consent doctrine and current Fourth Amendment jurisprudence would be internet-service providers' inability to provide the government with the contents of a message sent through e-mail without the sender's consent, since the internet-service provider acts as a transmitter of information, not as a receiver of it. The third-party doctrine does allow a receiver of an e-mail to disclose the contents of the e-mail to the government.

Constitutionally speaking, the result of *Clapper* should be the same regardless of whether current Fourth Amendment jurisprudence or the derivative-consent doctrine is used to sense its outcome. It is not a Fourth Amendment violation for telephone companies to disseminate metadata under the third-party doctrine. Telephone companies may also disseminate metadata under my derivative-consent doctrine because metadata is only level one surveillance, meaning that metadata is information that an individual consents to provide in order that the telephone company is able to complete the call.

The technological devices surrounding us are like windows into our lives. With proper use, they can be of great benefit to our economy,

social lives, and productivity. When these devices are misused by forces and individuals beyond our control, they can open windows into our lives, revealing intimate details in a manner not much different from the pervasive surveillance scheme found in George Orwell's classic dystopian novel *1984*.[199] The derivative-consent doctrine can close many of these open windows.

Of course, any time an individual interacts with another person, a company, or other third-party, whether in person or electronically, some information must be provided to facilitate the connection. These are windows into our lives that we can control, just like a person can open or close blinds. But when another entity tries to open the windows into your life without your permission,[200] the Fourth Amendment exists to quash these attempts and create balance. While a person hunched over their computer in a dark room with the blinds drawn and door locked may feel confident that the trail of websites he visits is known only to him, he is in for a rude awakening. But what confidence remains within him shall be placed in the individuals he communicates with. While the art of secret-keeping may not be highly valued in a society supercharged by the need for gossip, it is an art worth remembering for those you care about the most. The derivative-consent doctrine provides the needed Fourth Amendment protection that the content of our communication deserves. Finding the few friends trustworthy enough to guard our deepest and darkest secrets then becomes a higher priority than crouching in the shadows, hoping to devise a way to communicate remotely in a manner undetectable by our own government.

Alex Brown†

199. George Orwell, 1984 (1949).

200. Not including situations when one's presence in public allows others to physically follow or use devices to track your public position.

† This paper is dedicated to my parents, William and Dawn, my sister Aubree, grandparents Tom and Eleanor Raffle, and all the other friends and family who accompanied me, even if not always physically, on my journey through academia. I also want to thank Professor Lewis Katz for piquing my interest in Fourth Amendment issues through his Criminal Procedure I course. Finally, the staff of the Case Western Law Review deserve my thanks for the work they put into editing this paper.